

What is claimed is:

1. A method of performing quantum key distribution (QKD), comprising:
 - a) generating a random set of key bits $k_1, k_2, \dots, k_i \dots k_n$;
 - b) encrypting the key bits; and
 - c) using the encrypted key bits to form encrypted qubits.
2. The method of claim 1, including:
encrypting the key bits using a stream cipher.
3. The method of claim 2, wherein a password for the stream cipher is formed from a fraction of a QKD key.
4. The method of claim 2, including decoding the encrypted qubits by the stream cipher.
5. A method of performing quantum key distribution (QKD), comprising:
at a first QKD station:
 - a) generating a random set of key bits;
 - b) generating a pad by a stream cipher;
 - c) XOR-ing the key bits and the pad to obtain encrypted key bits; and
 - d) modulating weak optical pulses using the encrypted key bits to generate encrypted qubits.
6. The method of claim 5, further comprising at a second QKD station optically coupled to the first QKD station:
 - a) measuring the encrypted qubits using a random basis; and
 - b) recovering at least a subset of the key bits from the measured encrypted qubits by XOR-ing the measured encrypted qubits with the pad.
7. The method of claim 6, further including:
establishing a sifted key between the first and second QKD stations based on the key bits generated in the first QKD station and the key bits recovered in the second QKD station.

8. A QKD system, comprising:

a) a first QKD station having:

- a. an optical radiation source adapted to emit weak optical pulses of radiation;
- b. a first random number generator adapted to generate random numbers for use as first key bits;
- c. a first e/d module coupled to the first random number generator to encrypt the key bits thereby forming encrypted key bits;
- d. a polarization or phase modulator arranged to receive the weak optical pulses and adapted to modulate the polarization or phase of the weak optical pulses based on the encrypted key bits to form encrypted qubits;

b) a second QKD station optically coupled to the first QKD station and having:

- a. a second polarization or phase modulator adapted to receive and
- b. randomly modulate the encrypted qubits;
- c. a detector for detecting the modulated encrypted qubits; and
- d. a second e/d module coupled to the detector and adapted to recover from the modulated encrypted qubits second key bits corresponding to the first key bits.

9. A quantum cryptography system, comprising:

- a) a quantum key distribution (QKD) system that utilizes key bits and basis bits to encode weak optical pulses to form qubits; and
- b) a classical encryption system adapted to encode at least one of the key bits and the basis bits to form encrypted qubits.